What is claimed is:

1. A computerized method of transferring encrypted data between and among medical data management systems comprising:

recognizing data to be transmitted by a device;

determining a level of encryption dependent upon the nature of information to be transmitted by the device;

encrypting the data using a first secure key length for sensitive data;

encrypting the data using a second key length for remaining data; and

transmitting the data over a data communications media.

2. The method of claim 1 further comprising the steps of processing, using a secure key, a checksum of safety-critical data prior to transmitting the safety-critical data, and also comprising the step of transmitting the checksum after the step of transmitting the data over the data communications network.

3. The method of claim 2, further comprising the step of authenticating the integrity and source of the safety-critical data using the checksum.

4. The method of claim 1 wherein the data communications media over which data is transmitted is a data communications network.

5. The method of claim 4, wherein the data communications network is a public internetwork.

6. The method of claim 5, wherein the public network is the Internet.

7. An apparatus for variably encrypting and transferring medical data comprising:

a classifier having means for receiving an input of medical data from a medical device or a data management system, assigning a classification based upon what

the medical data represents, and outputting the classified medical data to a segregator;

a segregator having means for separating medical data into discrete data payloads according to the classification assigned the medical information by the classifier and outputting the segregated medical data to an encryptor;

an encryptor having means for variably encrypting segregated medical data based upon the level of security assigned to a particular payload of medical data and transmitting the variably encrypted data over a data communications media.

8. The apparatus of claim 7, wherein the means for variably encrypting and transferring of medical data can be implemented on various networks including the Internet and the World Wide Web.

9. The apparatus of claim 7, wherein the medical data comprises real-time data from patient monitoring equipment.

10. The apparatus of claim 9, wherein the patient monitoring equipment comprises an implantable medical device.

11. The apparatus of claim 7, wherein the means for assigning a classification based upon what the medical data represents assigns to real-time data from patient monitoring equipment a classification that will not be encrypted.

12. A network communications system linking an IMD to an information node via a secure medical information exchange network, comprising:

at least one key source in data communication with the IMD interface device and with the information node for transmitting an encryption key to the IMD interface device and a decryption key to the expert-data center;

an encryption engine residing within an IMD interface device for performing data modification information using the encryption key;

data communication means between the IMD interface and the medical information exchange network;

and a decryption engine residing within the information node having means to decrypt the encrypted sensitive information using the decryption key.

13. The network communications system of claim 12, wherein the information node is a clinician computer.

14. The network communications system of claim 12, wherein the information node is a remote expert system server.

15. The network communication system of claim 12, wherein the encryption engine is adapted to recognize non-real time data for encryption.

16. A network communications system for transmitting IMD instruction information from an information node to an IMD via a secure medical information exchange network, comprising:

at least one key source in data communication with the IMD interface device and with the information node for transmitting a decryption key to the IMD interface device and a encryption key to the information node;

data communication means between the IMD interface and the medical information exchange network;

an encryption engine residing within the information node having means for performing data modification of IMD instruction information; and

a decryption engine residing within an IMD interface device for performing data modification information for performing data integrity confirmation.

17. The network communications system of claim 16, wherein the key sources comprise hardware devices having keys hard coded into the IMD and IMD interface pair,

and a stored key source residing on the information node, respectively.

18. The network communications system of claim 16, wherein data transmitted from the information node comprises native data with an appended data integrity information.

19. The network communications system of claim 18, wherein the native data comprises IMD instructions.

20. The network communications system of claim 18, wherein the native data comprises IMD software upgrades.

21. The system of claim 12 or 16, wherein the IMD interface is in communication with an IMD implanted in a patient.

22. A computerized method of securely transferring data between an IMD and a remote information node over a computer network, the method comprising:

generating an encryption key for distribution to an IMD interface device;

generating a decryption key for distribution to the information node;

encrypting the sensitive information, transmitted from the IMD and residing on the IMD interface device, with the encryption key;

transferring the encrypted sensitive information from the IMD interface device to the remote information node, and

decrypting the encrypted information residing on the remote information node with the decryption key.

23. The method of claim 1 wherein said data to be transmitted includes one of and a combination of physiological data, cardiac data, neurological data, patient data, therapy data, diagnostic data and device data.

24. The method of claim 23 wherein said data to be transmitted is transferred based on differentiated encryption scheme.